

BF

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-040936

(43)Date of publication of application : 08.02.2002

(51)Int.Cl.

G09C 1/00

G06F 17/60

H04L 9/32

(21)Application number : 2000-224462

(71)Applicant : NTT ADVANCED TECHNOLOGY
CORP

(22)Date of filing : 25.07.2000

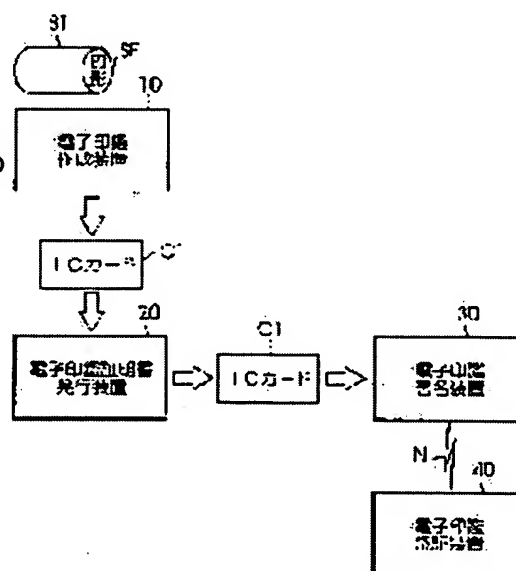
(72)Inventor : SHIRAISHI AKIRA

(54) ELECTRONIC SEAL GENERATION DEVICE, ELECTRONIC SEAL CERTIFICATE ISSUING DEVICE, ELECTRONIC SEAL SIGNING DEVICE, ELECTRONIC SEAL AUTHENTICATION DEVICE, AND SYSTEM AND METHOD FOR ELECTRONIC SIGNATURE

(57)Abstract:

PROBLEM TO BE SOLVED: To improve convenience for a person to handle an electronic document by using authentication by an electronic signature and visual recognition by a conventional signature and an imprint of a seal together, to certify the truth of the electronic document.

SOLUTION: An electronic seal generation device 10 reads an imprint SF of a seal ST as information on the imprint and records it in an IC card C1 for the imprint information together with a public key. An electronic seal certificate issuing device 20 gives a certificate provided with a certification seal proving that the imprint information and the public key stored in the IC card C1 are genuine, and records the certificate in the IC card C1. An electronic seal signing device 30 attaches the imprint information to the electronic document and also creates a signed document provided with a signature of the electronic document holder. An electronic seal authentication device 40 judges the truth or falsehood of the electronic document based on the signed document and the certificate, and makes it possible to visually authenticate the document by displaying the imprint information attached to the signed document and the imprint information included in the certificate.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-40936

(P2002-40936A)

(43)公開日 平成14年2月8日(2002.2.8)

(51)Int.Cl. ⁷	識別記号	F I	テマコード(参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 B 0 4 9
			6 4 0 Z 5 J 1 0 4
G 0 6 F 17/60	5 1 2	G 0 6 F 17/60	5 1 2
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 D

審査請求 未請求 請求項の数 8 O L (全 10 頁)

(21)出願番号 特願2000-224462(P2000-224462)

(22)出願日 平成12年7月25日(2000.7.25)

(71)出願人 000102739

エヌ・ティ・ティ・アドバンステクノロジー株式会社

東京都新宿区西新宿二丁目1番1号

(72)発明者 白石 旭

東京都新宿区西新宿二丁目1番1号 エヌ・ティ・ティ・アドバンステクノロジー株式会社内

(74)代理人 100064908

弁理士 志賀 正武

Fターム(参考) 5B049 AA05 AA06 EE09 FF01 GG00

5J104 AA07 AA09 AA16 EA04 KA01

KA16 LA03 LA06 NA02 NA35

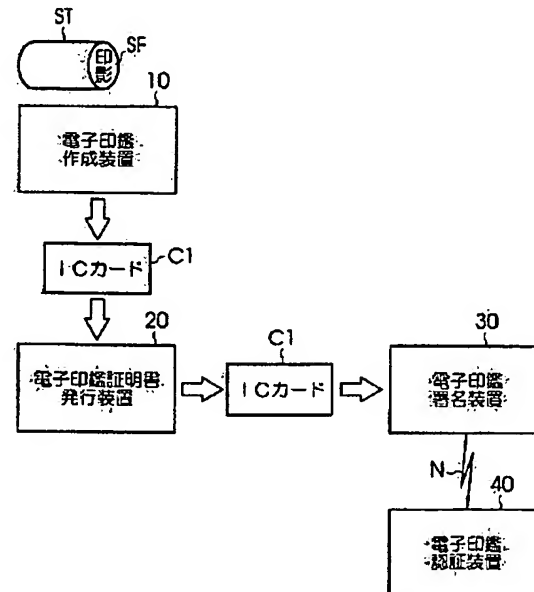
NA37 NA38

(54)【発明の名称】 電子印鑑作成装置、電子印鑑証明書発行装置、電子印鑑署名装置、及び電子印鑑認証装置、並びに電子署名システム及び電子署名方法

(57)【要約】

【課題】 電子文書の真偽を証明するに当たり、電子署名による認証と従来から用いられているサインや印影の目視による視認とを併用することによって、電子文書を取り扱う者の利便性を向上させる。

【解決手段】 電子印鑑作成装置10は印鑑STの印影SFを印影情報として読み取り印影情報用の公開鍵とともにICカードC1に記録する。電子印鑑証明書発行装置20は、ICカードC1に記録されている印影情報及び公開鍵が真正であることを証明する証明印を付した証明書を発行してICカードC1に記録する。電子印鑑署名装置30は、電子文書に対して印影情報を添付するとともに、電子文書の保持者の署名を付した署名文書を作成する。電子印鑑認証装置40は署名文書と証明書とに基づいて電子文書の真偽を判断し、署名文書に添付された印影情報と証明書に含まれる印影情報とを表示して目視による認証を可能とする。



【特許請求の範囲】

【請求項1】 印影を印影情報として読み取る印影読取部と、

前記印影情報用の公開鍵と秘密鍵とを対にして生成する印影情報用鍵生成部と、

前記印影情報と前記公開鍵とを対応づけるとともに、前記秘密鍵を付加した電子印鑑情報を作成する電子印鑑情報作成部と、

前記電子印鑑情報を電子印鑑に書き出す電子印鑑情報書出部とを具備することを特徴とする電子印鑑作成装置。

【請求項2】 少なくとも印影を示す印影情報と当該印影情報用に生成された公開鍵とが対応づけられて書き込まれている電子印鑑から、前記印影情報と前記公開鍵とを読み込む読込部と、

認証機関用の公開鍵と秘密鍵とを対にして生成する認証機関用鍵生成部と、

前記読込部から読み込んだ前記印影情報及び前記公開鍵に対して前記認証機関用の秘密鍵を用いて署名した証明印を付加した証明書を作成する証明書作成部とを具備することを特徴とする電子印鑑証明書発行装置。

【請求項3】 少なくとも認証機関用の秘密鍵を用いて署名が行われた印影を示す印影情報と前記印影情報用に作成された秘密鍵とが書き込まれている電子印鑑から前記印影情報と前記秘密鍵とを読み込む読込部と、

前記読込部から読み込んだ印影情報を電子文書に添付する印影添付部と、

前記印影が添付された電子文書に対して前記読込部から読み込んだ前記秘密鍵を用いて署名を行った署名文書を作成する署名部とを具備することを特徴とする電子印鑑署名装置。

【請求項4】 印影を示す印影情報が添付された電子文書に対して当該印影情報用の秘密鍵を用いて署名が行われた署名文書と、少なくとも前記印影情報と当該印影情報用に生成された公開鍵とが対応づけられてなる電子印鑑情報に対して認証機関用の秘密鍵を用いて署名が行われた署名印影情報とを読み込み、前記署名文書の署名と前記署名印影情報に含まれる前記印影情報用の公開鍵とに基づいて前記電子文書の認証を行う認証部と、前記署名文書に添付された印影情報と前記署名印影情報に含まれる印影情報とを表示する印影表示部とを具備することを特徴とする電子印鑑認証装置。

【請求項5】 印影を印影情報として読み取り、前記印影情報用に生成された対の公開鍵及び秘密鍵の内、当該公開鍵を前記印影情報に対応づけるとともに当該秘密鍵を付加した電子印鑑情報を作成して電子印鑑に書き出す電子印鑑作成装置と、

前記電子印鑑から前記印影情報と前記公開鍵とを読み込み、認証機関用に生成された対の公開鍵及び秘密鍵の内、当該秘密鍵を用いて前記印影情報及び前記公開鍵に対して署名した証明印を付加した証明書を作成し、前記

電子印鑑に書き込まれている前記印影情報及び前記公開鍵を前記証明書に更新する印鑑証明書発行装置とを具備することを特徴とする電子署名システム。

【請求項6】 前記電子印鑑に書き込まれた証明書から前記印影を示す印影情報を読み込んで電子文書に添付し、当該印影が添付された電子文書に対して前記電子印鑑から読み出した前記印影情報用の秘密鍵を用いて署名を行った署名文書を作成する電子印鑑署名装置と、

前記署名文書の署名と前記証明書に含まれる前記印影情報用の公開鍵とに基づいて前記電子文書の認証を行うとともに、前記署名文書に添付された印影情報と前記署名印影情報に含まれる印影情報とを表示する電子印鑑認証装置とを具備することを特徴とする請求項5記載の電子署名システム。

【請求項7】 印影を印影情報として読み取り、前記印影情報用に生成された対の公開鍵及び秘密鍵の内、当該公開鍵を前記印影情報に対応づけるとともに当該秘密鍵を付加した電子印鑑情報を作成して電子印鑑に書き出すステップと、

前記電子印鑑から前記印影情報と前記公開鍵とを読み込み、認証機関用に生成された対の公開鍵及び秘密鍵の内、当該秘密鍵を用いて前記印影情報及び前記公開鍵に対して署名した証明印を付加した証明書を作成し、前記電子印鑑に書き込まれている前記印影情報及び前記公開鍵を前記証明書に更新するステップとを有することを特徴とする電子署名方法。

【請求項8】 前記電子印鑑に書き込まれた証明書から前記印影を示す印影情報を読み込んで電子文書に添付し、当該印影が添付された電子文書に対して前記電子印鑑から読み出した前記印影情報用の秘密鍵を用いて署名を行った署名文書を作成するステップと、前記署名文書の署名と前記証明書に含まれる前記印影情報用の公開鍵とに基づいて前記電子文書の認証を行うとともに、前記署名文書に添付された印影情報と前記署名印影情報に含まれる印影情報とを表示するステップとを有することを特徴とする請求項7記載の電子署名方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、従来から用いられている印鑑の電子化を図った電子印鑑を作成する電子印鑑作成装置、従来から用いられている印鑑登録及び印鑑証明の電子化を図った電子印鑑証明書発行装置、文書に印鑑を捺印して行う署名の電子化を図った電子印鑑署名装置、及び文書の署名による文書の認証の電子化を図った電子印鑑認証装置、並びに電子署名システム及び電子署名方法に関する。

【0002】

【従来の技術】近年、インターネットを代表としてコンピュータネットワーク化が進み、電子化された各種の文書データの授受が一般的に行われている。ネットワーク

を介して文書データの授受は誰でもいつでも迅速に行うことができるため、極めて利便性が高い。よって、文書データのみならず、画像や音声等の各種データがネットワークを介して授受されると予想されている。

【0003】

【発明が解決しようとする課題】ところで、近年、電子政府プロジェクトの構成が予定されている。この電子政府プロジェクトは、各種申請書の電子化を図りインターネット等のネットワークを経由して各種申請手続きを行うものである。各種申請書の電子化が図られると、申請書に記載された情報にその個人の個性（例えば、筆跡等）が現れない。また、従来の窓口における対面業務と異なり、電子文書ではその電子文書が本人又は役所のものであるかの真偽が分からず、電子文書の内容が送信途中で改竄される虞がある等の危険性が指摘されている。

【0004】かかる危険性を回避するため、上述した電子政府プロジェクトにおいては、認証機関を通じた本人であることを証明するための「電子署名」を導入し、インターネット等のネットワークを介して送受信される申請書の真正さを担保することにより危険性を回避する予定である。ここで、電子署名は、公開鍵と秘密鍵との2つの鍵を用いる公開鍵方式による暗号化技術を応用したものであり、本人のみが所有する秘密鍵を用いて電子文書に付した署名を、本人の公開鍵を用いて確認するものである。このような電子署名を用いることにより電子文書の内容が改竄されていないことと、その電子文書は本人により作成されたことの2点を証明することができる。よって、認証に関する技術は電子政府プロジェクトの基盤となるものであり、極めて重要な役割を果たすこととなる。

【0005】しかしながら、旧来から法的効力を持つものとして利用されてきたサインや印影は、国民一般に広く浸透し、且つ慣習化しているため、電子文書の真偽の認証を電子的な署名のみによることは早急には国民一般に受け入れられないと考えられる。特に、サインや印影は本人及び窓口担当者の双方が同じものを容易に視認することができるものであるため、本人及び窓口担当者の双方が、本人が所有する印鑑を用いて捺印した申請書等の文書が窓口担当者へ渡され、又は役所が使用する印が捺印された文書が窓口担当者から本人へ渡されたことを確実に知ることができる。一方、電子署名の場合には、本人から窓口担当者へ又は窓口担当者から本人へ渡された文書には本人の電子署名が付されているか、又は役所が使用している署名であるかを確認することは極めて困難である。

【0006】本発明は上記事情に鑑みてなされたものであり、電子文書の真偽を証明するに当たり、電子署名による認証と従来から用いられているサインや印影の目視による視認とを併用することによって、電子文書を取り扱う者の利便性を向上させることができる電子印鑑作成

装置、電子印鑑証明書発行装置、電子印鑑署名装置、及び電子印鑑認証装置、並びに電子署名システム及び電子署名方法を提供することを目的とする。

【0007】

【課題を解決するための手段】上記課題を解決するために、本発明の電子印鑑作成装置は、印影を印影情報として読み取る印影読取部と、前記印影情報用の公開鍵と秘密鍵とを対にして生成する印影情報用鍵生成部と、前記印影情報と前記公開鍵とを対応づけるとともに、前記秘密鍵を付加した電子印鑑情報を作成する電子印鑑情報作成部と、前記電子印鑑情報を電子印鑑に書き出す電子印鑑情報書出部とを具備することを特徴としている。また、本発明の電子印鑑証明書発行装置は、少なくとも印影を示す印影情報と当該印影情報用に生成された公開鍵とが対応づけられて書き込まれている電子印鑑から、前記印影情報と前記公開鍵とを読み込む読込部と、認証機関用の公開鍵と秘密鍵とを対にして生成する認証機関用鍵生成部と、前記読込部から読み込んだ前記印影情報及び前記公開鍵に対して前記認証機関用の秘密鍵を用いて署名した証明印を付加した証明書を作成する証明書作成部とを具備することを特徴としている。また、本発明の電子印鑑署名装置は、少なくとも認証機関用の秘密鍵を用いて署名が行われた印影を示す印影情報と前記印影情報用に作成された秘密鍵とが書き込まれている電子印鑑から前記印影情報と前記秘密鍵とを読み込む読込部と、前記読込部から読み込んだ印影情報を電子文書に添付する印影添付部と、前記印影が添付された電子文書に対して前記読込部から読み込んだ前記秘密鍵を用いて署名を行った署名文書を作成する署名部とを具備することを特徴としている。また、本発明の電子印鑑認証装置は、印影を示す印影情報が添付された電子文書に対して当該印影情報用の秘密鍵を用いて署名が行われた署名文書と、少なくとも前記印影情報と当該印影情報用に生成された公開鍵とが対応づけられてなる電子印鑑情報に対して認証機関用の秘密鍵を用いて署名が行われた署名印影情報とを読み込み、前記署名文書の署名と前記署名印影情報に含まれる前記印影情報用の公開鍵とに基づいて前記電子文書の認証を行う認証部と、前記署名文書に添付された印影情報と前記署名印影情報に含まれる印影情報とを表示する印影表示部とを具備することを特徴としている。本発明の電子署名システムは、印影を印影情報として読み取り、前記印影情報用に生成された対の公開鍵及び秘密鍵の内、当該公開鍵を前記印影情報に对应づけるとともに当該秘密鍵を付加した電子印鑑情報を作成して電子印鑑に書き出す電子印鑑作成装置と、前記電子印鑑から前記印影情報と前記公開鍵とを読み込み、認証機関用に生成された対の公開鍵及び秘密鍵の内、当該秘密鍵を用いて前記印影情報及び前記公開鍵に対して署名した証明印を付加した証明書を作成し、前記電子印鑑に書き込まれている前記印影情報及び前記公開鍵を前記証明書

に更新する印鑑証明書発行装置とを具備することを特徴としている。また、本発明の電子署名システムは、前記電子印鑑に書き込まれた証明書から前記印影を示す印影情報を読み込んで電子文書に添付し、当該印影が添付された電子文書に対して前記電子印鑑から読み出した前記印影情報用の秘密鍵を用いて署名を行った署名文書を作成する電子印鑑署名装置と、前記署名文書の署名と前記証明書に含まれる前記印影情報用の公開鍵とに基づいて前記電子文書の認証を行うとともに、前記署名文書に添付された印影情報と前記署名印影情報に含まれる印影情報とを表示する電子印鑑認証装置とを具備することを特徴としている。また、本発明の電子署名方法は、印影を印影情報として読み取り、前記印影情報用に生成された対の公開鍵及び秘密鍵の内、当該公開鍵を前記印影情報に対応づけるとともに当該秘密鍵を付加した電子印鑑情報を作成して電子印鑑に書き出すステップと、前記電子印鑑から前記印影情報と前記公開鍵とを読み込み、認証機関用に生成された対の公開鍵及び秘密鍵の内、当該秘密鍵を用いて前記印影情報及び前記公開鍵に対して署名した証明印を付加した証明書を作成し、前記電子印鑑に書き込まれている前記印影情報及び前記公開鍵を前記証明書に更新するステップとを有することを特徴としている。また、前記電子印鑑に書き込まれた証明書から前記印影を示す印影情報を読み込んで電子文書に添付し、当該印影が添付された電子文書に対して前記電子印鑑から読み出した前記印影情報用の秘密鍵を用いて署名を行った署名文書を作成するステップと、前記署名文書の署名と前記証明書に含まれる前記印影情報用の公開鍵とに基づいて前記電子文書の認証を行うとともに、前記署名文書に添付された印影情報と前記署名印影情報に含まれる印影情報とを表示するステップを有することを特徴としている。

【0008】

【発明の実施の形態】以下、図面を参照して本発明の一実施形態による電子印鑑作成装置、電子印鑑証明書発行装置、電子印鑑署名装置、及び電子印鑑認証装置、並びに電子署名システム及び電子署名方法について詳細に説明する。尚、以下の説明では印鑑の印影を用いる場合を例に挙げて説明する。しかしながら、本発明はサインの場合にも適用が可能である。つまり、本明細書で用いられる語句「印影」とは、印鑑の印影のみならずサイン等を含む意味である。

【0009】〔電子署名システム〕図1は、本発明の一実施形態による電子署名システムの全体構成を示すブロック図である。以下、図面を参照して本発明の電子署名システムの構成及び動作の概要について説明する。図1に示したように、本発明の一実施形態による電子署名システムは、電子印鑑作成装置10、電子印鑑証明書発行装置20、電子印鑑署名装置30、及び電子印鑑認証装置40を含んで構成される。

【0010】電子印鑑作成装置10は、例えば印鑑STの販売店に配置され、印鑑STの印影SFを印影情報として読み取るとともに印影情報用の公開鍵及び秘密鍵を生成する。そして、読み取った印影情報と作成した公開鍵とを対応づけるとともに生成した秘密鍵を付加した電子印鑑情報を作成して電子印鑑としてのICカードC1に書き出す。電子印鑑作成装置10の役割は、従来の印鑑作成に相当する。

【0011】電子印鑑証明書発行装置20は、区役所、市役所、第三者機関、その他の認証機関に配置され、ICカードC1に記録されている電子印鑑情報がICカードC1の保持者のものであることを証明する証明書を発行する。ICカードC1の保持者は運転免許書やパスポート等の身分証明書とともにICカードC1を公的機関に提出して証明書を発行してもらう。電子印鑑証明書発行装置20は発行した証明書を既に記録されている印影情報及び公開鍵に代えてICカードC1に書き出す。

ICカードC1に記録される証明書は従来の印鑑証明書に相当し、電子印鑑証明書発行装置20の役割は、従来の印鑑登録と印鑑証明書の発行に相当する。このICカードC1はいわば証明書入りの電子的な印鑑として利用される。

【0012】電子印鑑署名装置30は、例えばICカードC1の保持者の自宅に配置されたパーソナルコンピュータによって実現され、ICカードC1に書き込まれている証明書から印影情報を読み込み、読み込んだ印影情報をICカードC1の保持者が作成した電子文書に対して添付する。また、ICカードC1に記録されている秘密鍵を用いて印影情報が添付された電子文書に対する署名としての電子署名を生成する。このように、電子印鑑署名装置30は、ICカードC1の保持者が作成した電子文書に対して公的機関の認証を受けた証明書に含まれる印影情報を添付し、その保持者の電子署名を付した署名文書を作成する。電子印鑑署名装置30の役割は、従来の文書への捺印に相当する。電子印鑑署名装置30はインターネット等のネットワークNを介して電子印鑑認証装置40と接続され、署名文書とともに証明書を電子印鑑認証装置40へ送信する。

【0013】電子印鑑認証装置40は、例えば区役所、市役所、その他の行政機関に配置され、ネットワークNを介して送信されてきた証明書に含まれる印影情報用に生成された公開鍵を用いてネットワークNを介して送信されてきた署名文書に添付された電子署名の真偽を判断することにより電子文書の認証を行う。また、電子印鑑認証装置40は、署名文書中の電子文書に添付された印影情報と証明書に含まれる印影情報とをCRT (Cathode Ray Tube) 等の表示装置に表示する。この表示装置に表示された印影情報を目視して行政機関の役人がその真偽を判断して電子文書を認証する。

【0014】印鑑STの保持者が電子文書を作成する際

に、印鑑S Tの印影S Fをスキャナ等を用いて読み込み、この印影情報を添付した電子文書として作成すれば、行政機関の役人がその真偽を目視して判断することが可能であり、従来から行われている目視による認証をも行うことができると考えられる。しかしながら、単に印影情報を電子文書に添付するだけでは、電子文書に添付された印影情報は容易に流用及び改竄が可能である。従って、電子文書に添付された印影情報が改竄された場合にはその電子文書の真正を保証することができず、流用された場合には悪用される虞がある。

【0015】これに対し、本発明の一実施形態による電子署名システムは、上述したように印影S Fの印影情報を電子署名の認証に利用される公開鍵と同様に、信用のおける認証機関が署名した証明書として発行してもらい、この証明書付きの印影情報を電子文書に添付している。これにより、電子署名で保証された文書の真正を、印影による目視によっても証明することができるようになり、これまで慣習となっていた印影による文書の真正の証明手段としての親和性を確保することができる。

【0016】尚、以上説明した本発明の一実施形態による電子署名システムにおいては、電子印鑑作成装置10が印鑑S Tの販売店に配置され、電子印鑑証明書発行装置20は、区役所、市役所、第三者機関、その他の認証機関に配置され、各々が別々に設けられている場合を例に挙げて説明した。しかしながら、電子印鑑作成装置10及び電子印鑑証明書発行装置20をともに、例えば区役所、市役所等の行政機関に配置すれば、印鑑S Tと身分証明書とを行政機関に持っていくだけで、電子印鑑の作成、印鑑登録、及び印鑑証明書作成を行うことができる。

【0017】以上、本発明の一実施形態による電子署名システムの全体構成について説明したが、次に電子署名システムに含まれる本発明の一実施形態による電子印鑑作成装置、電子印鑑証明書発行装置、電子印鑑署名装置、及び電子印鑑認証装置について詳細に説明する。

【0018】〔電子印鑑作成装置〕図2は、本発明の一実施形態による電子印鑑作成装置10の構成を示すブロック図である。図2に示したように、電子印鑑作成装置10は、印影読み取り部12、鍵生成部14、電子印鑑情報作成部16、及び書き出し部18を含んでなる。印影読み取り部12は、例えばイメージスキャナ等によって実現され、印鑑S Tの印影S Fを印影情報F 1として読み取る。鍵生成部14は、印影情報F 1用の公開鍵OK 1と秘密鍵SK 1とを対にして生成する。

【0019】電子印鑑情報作成部16は、印影読み取り部12で読み取った印影情報F 1と鍵生成部14で生成された印影情報F 1用の公開鍵OK 1とを対応づけるとともに、鍵生成部14で生成された印影情報F 1用の秘密鍵SK 1を付加した電子印鑑情報を作成する。書き出し部18は、電子印鑑情報作成部16で作成された電子

印鑑情報をICカードC 1へ書き出す。以上の処理によって電子印鑑としてのICカードC 1が作成される。

尚、図2においては、印鑑S Tの印影S Fを読み取る場合を例に挙げて説明したが、印影S Fに代えて手書きのサインを印影情報とした電子印鑑情報を作成する場合にも適用することができる。

【0020】〔電子印鑑証明書発行装置〕次に、本発明の一実施形態による電子印鑑証明書発行装置20について詳細に説明する。図3は、本発明の一実施形態による電子印鑑証明書発行装置20の構成を示すブロック図である。尚、図3においては、説明の便宜のためICカードC 1を2つ図示しているが、これらは物としては同一であり内部に記憶される情報のみが異なる。

【0021】図3に示したように、本発明の一実施形態による電子印鑑証明書発行装置20は、入出力部22、鍵生成部24、情報入力部26、及び証明書作成部28を含んでなる。入出力部22は、電子印鑑としてのICカードC 1に対して任意の情報の読み込み、書き出し、及び更新ができる。この入出力部22は読込部を含んでなす。鍵生成部24は、ICカードC 1に記憶されている公開鍵OK 1と印影情報F 1とが、印鑑S Tの保持者のものであることを証明する証明印S 1を生成するために用いる認証機関用の一対の公開鍵OK 2と秘密鍵SK 2とを生成する。

【0022】この公開鍵OK 2と秘密鍵SK 2とはICカードC 2に書き出される。尚、本実施形態においては公開鍵OK 2と秘密鍵SK 2とがICカードC 2に書き出される場合を例に挙げて説明するが、必ずしもICカードC 2に書き出す必要はなく、他の記録媒体（例えば、フレキシブルディスク、ハードディスク、光磁気ディスク、CD-R、CD-RW、DVD-R、DVD-RW等）に書き出すようにしても良い。また、公開鍵OK 2は例えばインターネット等のネットワークを介して何人も入手することが可能である。

【0023】上記証明印S 1は一種の電子署名であり、鍵生成部24が生成した秘密鍵SK 2を用いて生成される。上述したように、公開鍵OK 2は何人も入手することができるため何人も証明印S 1の内容を見ることができが、秘密鍵SK 2が公開されていないため、例えばその内容を見ることができたとしても証明印S 1を作成することはできない。情報入力部26は、例えばキーボード等により実現され、証明書の有効期限等を示す証明書情報P 1を入力する。

【0024】証明書作成部28は、秘密鍵SK 2を用いて署名した証明印S 1を作成し、入出力部22を介してICカードC 1から読み込んだ公開鍵OK 1、印影情報F 1、及び証明書情報P 1に対して作成した証明印S 1を付した証明書CRを作成する。ここで、証明書CR中の公開鍵OK 1及び印影情報F 1は秘密鍵SK 2を用いて署名した証明印S 1が付加されており、これは署名印

影情報に相当するものである。この証明書CRは入出力部22を介してICカードC1に書き出される。尚、このとき、入出力部22は、先に記録されていた公開鍵OK1及び印影情報F1を証明書CRに更新する。以上の処理によって証明書入りの電子的な印鑑が作成される。

【0025】〔電子印鑑署名装置〕次に、本発明の一実施形態による電子印鑑署名装置30について詳細に説明する。図4は、本発明の一実施形態による電子印鑑署名装置30の構成を示すブロック図である。図4において、ICカードC1は図3に示した電子印鑑証明書発行装置20が発行した証明書CRが記録されたICカードである。

【0026】図4に示したように、本発明の一実施形態による電子印鑑署名装置30は、情報読み込み部32、印影添付部34、署名部36、及び通信部38を含んでなる。情報読み込み部32は、ICカードC1に記録されている証明書CR及び印影情報用の秘密鍵SK1を読み込む。印影添付部34は、ICカードC1の保持者が別途作成した電子文書Dに対して、証明書CRに含まれる印影情報F1を添付する。

【0027】署名部36は、秘密鍵SK1を用いて電子文書Dの作成者の署名を作成し、印影情報F1が添付された電子文書Dに付加した署名文書SDを作成する。通信部38は、署名部36が作成した署名文書を証明書CRとともにインターネット等のネットワークNへ送出する。以上の処理によって、ICカードC1に記録された印影情報F1が添付された電子文書Dに、ICカードC1の保持者の署名が付加された署名文書SDが証明書CRとともにネットワークを介して送信される。

【0028】〔電子印鑑認証装置〕次に、本発明の一実施形態による電子印鑑認証装置40について詳細に説明する。図5は、本発明の一実施形態による電子印鑑認証装置40の構成を示すブロック図である。図5に示したように、電子印鑑認証装置40にはネットワークNを介して署名文書SDと証明書CRとが送信されてくる。かかる署名文書SD及び証明書CRにより認証を行うために、電子印鑑認証装置40は、通信部42、認証部44、及び印影表示部46を備える。尚、図5においては、証明書CRが署名文書SDとともにネットワークNを介して送信されてくる様子を示すとともに、証明書CR中のどの情報が認証に用いられるかを明確化するために、証明書CRを2つ図示している。

【0029】通信部42は、ネットワークNを介して授受される各種情報の通信制御を行う。認証部44は、証明書CR中に含まれる公開鍵OK1を用いて電子署名S2を含む署名文書SDが真正のものであるか否かの認証を行う。つまり、署名文書SDに含まれる電子署名S2は、図4を用いて説明したようにICカードC1に含まれる秘密鍵SK1によって作成されたものであるため、公開鍵OK1を用いれば電子署名S2の内容を確認する

ことができ、よって電子署名S2の真偽を判断することによって、電子文書Dが真正のものであるか否かを認証することができる。印影表示部46は、電子文書Dに添付されている印影情報F1と、証明書証明書CRに含まれる印影情報をCRT等の表示装置に表示する。

【0030】このように、電子印鑑認証装置40は、認証部44によって電子文書Dに付された電子署名S2の真偽によって電子文書Dが真正のものであるか否かを判断している。また、印影表示部46によって電子文書Dに付された印影情報F1と証明書CRに含まれる印影情報F1とを表示している。従って、電子文書Dが真正のものであるか否かの認証を行う際に、電子署名を用いて機械的に行うとともに、従来から行われている視認による認証を行うことができる。尚、印影表示部46が電子文書Dに添付されている印影情報F1を表示する際には、電子文書Dに添付されている印影情報F1のみを表示しても良く、印影情報F1が付された状態での電子文書Dを表示するようにしても良い。

【0031】〔電子署名方法〕以上、本発明の一実施形態による電子署名システムを構成する本発明の一実施形態による電子印鑑作成装置、電子印鑑証明書発行装置、電子印鑑署名装置、及び電子印鑑認証装置について説明したが、次に電子署名システムの動作、つまり電子署名方法について詳細に説明する。

【0032】まず、電子印鑑としてのICカードC1を作成する場合には印鑑の販売店へ出向き印鑑STを選択する。そして、電子印鑑作成装置10によって選択した印鑑STの印影SFを読み取らせる。読み取られた印影情報F1は鍵生成部14で生成された公開鍵OK1と対応づけられ、更に鍵生成部14で生成された秘密鍵SK1が付加されて電子印鑑情報としてICカードC1に書き出される。このようにして電子印鑑としてのICカードC1が生成されたので、選択した印鑑STと生成したICカードC1との代金を支払って購入する。

【0033】ICカードC1の保持者はICカードC1と身分証明書とを持参して認証機関へ出向き、認証機関の窓口担当者にICカードC1と身分証明書を差し出し、身分証明書によって窓口担当者に本人であることの確認をもらった上で、ICカードC1内に証明書CRを作成してもらう。電子印鑑証明書発行装置20にICカードC1が挿入されると、入出力部22は、ICカードC1から公開鍵OK1及び印影情報F1を読み込む。また、情報入力部26からは有効期限等の証明書情報P1が入力される。

【0034】証明書作成部28は、鍵生成部24が生成した秘密鍵SK2を用いて署名した証明印S1を作成し、入出力部22を介してICカードC1から読み込んだ公開鍵OK1、印影情報F1、及び証明書情報P1に対して作成した証明印S1を付した証明書CRを作成する。この証明書CRは入出力部22を介してICカード

C1に書き出され、先に記憶されている公開鍵OK1及び印影情報F1の更新がなされる。尚、証明書CRには電子印鑑証明書発行装置20の鍵生成部24で生成された秘密鍵SK2を用いて作成された証明印S1が付されている。よって、証明印S1の内容を見ることはできるが、例えば印影情報F1を取り替えて偽の証明書CRを作成することはできない。以上の処理を終えたICカードC1はICカードC1の保持者に身分証明書とともに返却される。

【0035】ICカードC1の保持者が自ら作成した電子印鑑を用いて捺印する場合には、ICカードC1を電子印鑑署名装置30に差し込む。ICカードC1の保持者が印影情報F1を添付する電子文書Dを指定すると、ICカードC1から証明書CRに含まれる印影情報F1が読み込まれ、印影添付部34が指定された電子文書Dに印影情報F1が添付される。次に、ICカードC1から印影情報F1用に生成された秘密鍵SK1が読み込まれ、署名部36がこの秘密鍵SK1を用いて電子署名S2を作成し、印影情報F1が付された電子文書Dに電子署名S2を付した署名文書SDを作成する。

【0036】この電子文書SDは、ICカードC1の保持者の秘密鍵SK1を用いて作成された電子署名S2が付されており、例え第三者がその内容を見ることはできても、秘密鍵SK1は、ICカードC1内に格納されているため、ICカードC1の保持者以外の者が電子署名S2と同一の電子署名を作成することはできない。よって、電子文書Dや印影情報F1の内容が改竄して電子署名S2と同一の電子署名を付した署名文書SDを作成することはできない。従って、電子署名S2によって電子文書Dの真正さを担保することができる。

【0037】ICカードC1の保持者が作成した署名文書SDを行政機関等に送信する場合には、保持者は署名文書SDの送信指示を行う。かかる送信指示がなされると、署名文書SDとともに証明書CRがネットワークに送信される。署名文書SDと証明書CRとは別個に送信される訳ではなく一対にして送信される。署名文書SDと証明書CRとがネットワークNを介して送信されてくると、電子署名S2が添付された電子文書Dが真正のものであるか否かが認証部44によって判断されるとともに、印影表示部46によって電子文書Dに付された印影情報F1と証明書CRに含まれる印影情報F1とが表示される。従って、電子文書Dが真正のものであるか否かの認証を行う際に、電子署名を用いて機械的に行うとともに、従来から行われている視認による認証を行うことができる。

【0038】以上、本発明の一実施形態による電子印鑑作成装置、電子印鑑証明書発行装置、電子印鑑署名装置、及び電子印鑑認証装置、並びに電子署名システム及び電子署名方法について説明したが、本発明は上記実施形態に制限されることなく、本発明の範囲内において

自由に変更が可能である。例えば、上記実施形態においては、電子印鑑認証装置40が備える印影表示部46によって電子文書Dに付された印影情報F1と証明書CRに含まれる印影情報F1とを単に表示するだけであったが、電子文書Dに付された印影情報F1と証明書CRに含まれる印影情報F1とのパターンが一致するか否かを判断する判断部を設けて目視による認証を自動化してもよい。更に、ICカードC1に記録される印影情報F1を圧縮して記録に要する容量の低減を図ってもよい。

尚、かかる場合には圧縮された印影情報F1の目視が必要となる電子印鑑署名装置30及び電子印鑑認証装置40に圧縮された印影情報F1を伸長して復元する復元部を設ける必要がある。

【0039】

【発明の効果】以上、説明したように、本発明によれば、電子署名による電子文書の真正の認証と、電子文書に添付された印影によって文書の真正の認証とを並行して行うことができるという効果がある。また、電子文書に添付される印影情報は、電子文書に添付される電子署名を作成する際に利用される公開鍵とともに認証機関の認証を受けたものであり、この認証機関の認証を受けた証明書を用いて電子文書に添付された印影情報が真正のものであるか否かが判断される。よって、仮に電子文書に添付された印影情報が偽造されて別の印影情報が添付されていたとしても、電子文書に添付された印影情報と証明書に含まれる印影情報とが異なるため、偽造を知ることが可能になるという効果がある。

【図面の簡単な説明】

【図1】 本発明の一実施形態による電子署名システムの全体構成を示すブロック図である。

【図2】 本発明の一実施形態による電子印鑑作成装置10の構成を示すブロック図である。

【図3】 本発明の一実施形態による電子印鑑証明書発行装置20の構成を示すブロック図である。

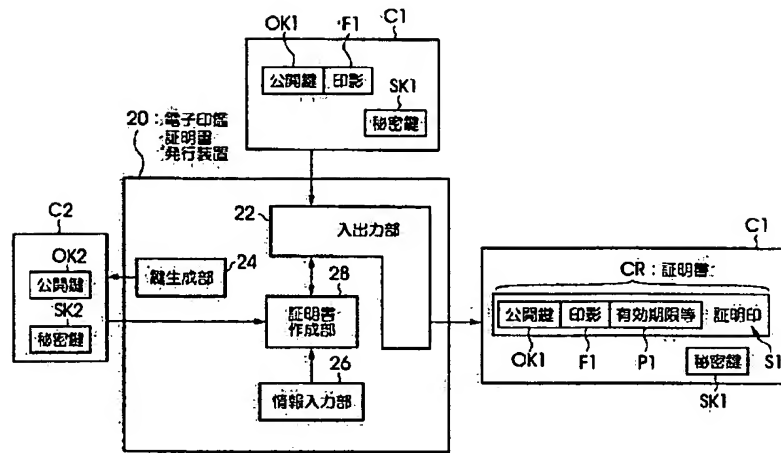
【図4】 本発明の一実施形態による電子印鑑署名装置30の構成を示すブロック図である。

【図5】 本発明の一実施形態による電子印鑑認証装置40の構成を示すブロック図である。

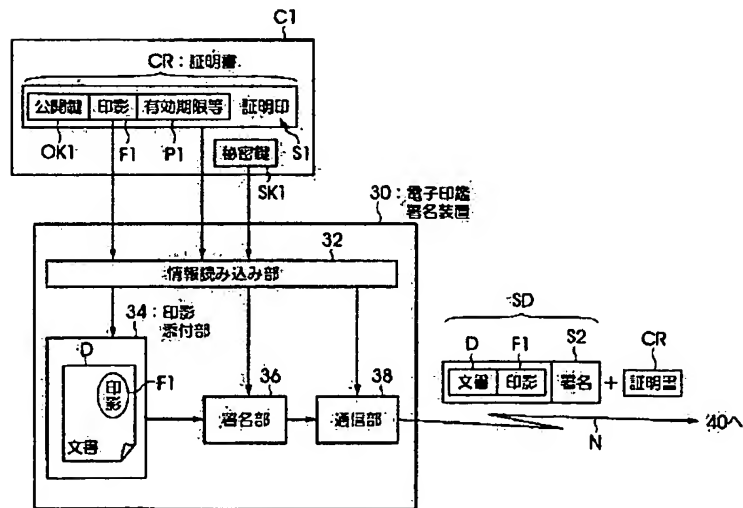
【符号の説明】

- | | |
|----|------------------|
| 10 | 電子印鑑作成装置 |
| 12 | 印影読み取り部（印影読取部） |
| 14 | 鍵生成部（印影情報用鍵生成部） |
| 16 | 電子印鑑情報作成部 |
| 18 | 書き出し部（電子印鑑情報書出部） |
| 20 | 電子印鑑証明書発行装置 |
| 22 | 入出力部（読込部） |
| 24 | 鍵生成部（認証機関用鍵生成部） |
| 28 | 証明書作成部 |
| 30 | 電子印鑑署名装置 |
| 32 | 情報読み込み部（読込部） |

【図3】



【図4】



【図5】

